Quantum Paradox: Redefining Secure Communication with Quantum and Post-Quantum Cryptographic Breakthroughs

B.D.Anuththara Divyanjalie Hettiarachchi
Department of Computer Science
Sri Lanka Institute of
Information Technology
Colombo, Sri Lanka
anuththara325@gmail.com

***Abstract*—The rise of quantum computing brought unparalleled challenges to traditional cryptography and turned secure communication into a paradox. This review outlines the efforts of quantum and post-quantum cryptography in addressing these security concerns. Quantum cryptography secures communications with principles of quantum mechanics that are, for essential reasons, impossible to break, with special reference to quantum key distribution. In turn, post-quantum cryptography enables the algorithms that provide resistance against quantum attacks yet operate within the classical framework. Major achievements range from deployment and standardization efforts over advances in the field of quantum key distribution to the development of post-quantum cryptography. These advances face a range of scalability challenges, issues in computational efficiency, and practical implementation. The review further points to the development of hybrids that incorporate quantum with post-quantum schemes to enhance security in the quantum era and to offer forward-looking secure communication solutions.**

***Index Terms*—Quantum Cryptography, Post-Quantum Cryptography, Secure Communications, Quantum Computing, Cryptographic Breakthroughs**

I. Introduction

In the dynamic regime of information security, a paradox is unraveled that will alter the very fabric of how most sensitive information will be secured. This is the story of the quantum paradox. This one phenomenon is regarded as the biggest threat and the most formidable defense in history to secure communications. Imagine waking one morning to a world where all encrypted e-mails, secure financial transactions, and privileged government communications are suddenly and totally in the public domain. Not the plot of a techno-thriller but an impending reality in the world of information security, and the culprit is identified as quantum computing—a new, revolutionary technology that threatens to break through the cryptographic shields that have long protected digital secrets [1]. Rooted in the ideas of quantum physics, quantum computing is considered an advanced form of computation that can speedily and efficiently attack particularly challenging scenarios [1]. Even before all the quantum machines are put to work, some very profound impacts on global progress may be had by quantum technology [1]. For decades, difficult mathematical problems have been relied upon to develop encryption algorithms that safeguard data by information security professionals. The bedrock of modern cybersecurity, these algorithms have survived both time and the power of computing—until now [1]. A new turn in evolution to practical tools is being taken by quantum computers, and with them, the power to solve such mathematical puzzles in just minutes has been possessed, making current methods of encryption obsolete.

That is where the paradox is played out. The very quantum principles threatening current information security paradigms are promised to offer unprecedented protection. Quantum cryptography is recognized as a method of encryption in which data protection and transport are made possible due to the inherent properties of quantum mechanics [2]. The process of encrypting data such that it may be decoded only by the owner of the correct secret key is known as cryptography [2]. Quantum cryptography differs from the traditional methods of cryptography by depending not on mathematics but on physics when it comes to security [2]. The power of quantum mechanics is harnessed by exploiting its counterintuitive and very unique properties, and quantum cryptography has emerged to hold out the prospect of providing communication channels that are essentially immune to any form of interception or eavesdropping [2]. Consequently, it has become, in many respects, both a universal lockpick and an unbreakable lock from the very same source. Information security is being pushed to an interesting juncture in some sense: post-quantum cryptography is already being developed by cryptography developers and security experts, with new kinds of cryptosystems impervious to traditional computing and quantum computing methods being researched [3]. Depending on the fundamental issue that the security is based on, the cryptosystems are separated into multiple families. Both classical and quantum computers are thought to be unable to solve these fundamental problems [3]. Classical algorithms robust enough to withstand

quantum attacks are being researched, while on the other hand, the usage of quantum principles themselves is being researched to create new, unbreakable methods of encryption. The role of quantum computing in this regard is considered immense. Essentially, calculations are carried out at a rate beyond that achievable with a classical computer by using the superposition and entanglement of quantum mechanics [1]. The mathematical principles behind today's cryptographic systems are apparently put at risk by this exponential increase in computational power. Consider the Rivest-Shamir-Adleman (RSA) algorithm, which is in wide use and whose security depends on the hardness of the factorization problem of large numbers [4]. If Shor's algorithm is applied by a strong enough quantum computer, then such numbers could be factored into a polynomial time [4]. Similarly, elliptic curve cryptography, another backbone of modern secure communications, may be proved vulnerable to quantum attacks [5]. This looming threat has galvanized the cybersecurity community into action, spurring the development of two main lines of defense. First, a process dependent on the very principles of quantum mechanics is recognized as quantum cryptography to yield—theoretically, at least—completely unbreakable encryption. For instance, quantum key distribution (QKD) is a process whereby a shared random secret key used in symmetric encryption and decryption of messages can be generated by parties [6]. The second approach pertains to the development of post-quantum cryptography. The aim is to find novel algorithms that are resistant not only to quantum but also to classic attacks, using mathematical problems that, most likely, are impossible to solve in a reasonable amount of time even for quantum computers [7]. Some of the promising candidates in this area are lattice-based cryptography, hash-based signatures, and code-based cryptography [7].

The race now is to develop and install these new cryptographic methods, which are by no means regarded as an academic exercise. The effort is reflected as an enterprise that is critical in its nature and has large implications for national security, economic stability, and personal privacy in the digital age. The core of the quantum paradox in information security is delved into by this literature review. The debate is focused on how the cybersecurity landscape is being transformed by the quantum advent through the observation of threats to the existing encryption standards, with reviews of the revolutionary security solutions that are allowed. The complex web of technologies poised to redefine secure communications will be unwound by the review, right from quantum key distribution to post-quantum cryptography. In this paper, an overview of the current research, including emerging trends, is presented to enable knowledge of the opportunities and difficulties in information security that are posed by quantum and post-quantum encryption. The future of digital asset protection and, in turn, communications with regard to the information security era depend on one's understanding and leveraging quantum and post-quantum cryptography. This review gives an overview, therefore, of the challenges presented, the opportunities availed by this paradigm shift, and the implications of such regarding how the information security community works to outsmart a world that will be increasingly quantum. Research into these leading-edge technologies and methodologies throws light on the effort to protect sensitive information against new quantum threats while turning to the very power of quantum principles to grant increased security measures.

II. Research Objectives

A. Evaluate the Impact of Quantum Computing on Classical Cryptographic Systems

A significant impact on classical cryptosystems is being caused by the rapid advancement of quantum computing. As quantum computers continue to advance, most shared encryption algorithms are expected to become obsolete. The vulnerabilities in classical cryptography due to quantum computing's capabilities are aimed to be analyzed by this review, highlighting how existing security protocols could be disrupted and how the understanding of secure communication in a quantum-enabled future could be reshaped.

B. Assess the Viability and Limitations of Quantum Cryptography

A secure channel for communication is promised by quantum cryptography, and more so by QKD, but quite a number of challenges are found in its practical implementation. An attempt is being made by this literature review to ascertain the current status of quantum cryptographic technologies, their effectiveness in real life, and what is preventing wide practical applications. Discussions will be made on technological, logistical, and regulatory barriers in the use of quantum cryptography and what role QKD will play in the future of secure communications.

C. Analyze the Development and Standardization of Post-Quantum Cryptographic Algorithms

Different types of post-quantum cryptographic algorithms, like lattice-based schemes, hash-based schemes, and code-based ones, are discussed in this review, along with their strengths and weaknesses, their defense against quantum attacks, and the level of standardization. The various challenges of migrating organizations from classical systems to post-quantum cryptography are also examined to reach a robust security framework for the future.

D. Investigate the Synergies Between Quantum and Post-Quantum Cryptographic Approaches

The possible interactions of quantum and post-quantum cryophysics are discussed in this study in a manner to form hybrid systems by merging quantum techniques like QKD with post-quantum algorithms to enhance general security in communication infrastructures. Collaborative opportunities to develop new countermeasures against quantum threats are explored.

III. Review Methodology

The systematic approach was adopted for conducting this review with the aid of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework [8] in a manner that will enable the comprehensive and unbiased summarization of the literature on quantum and post-quantum cryptography within the context of secure communications.

A. Search Strategy

A structural search was performed in several academic databases, such as IEEE Xplore and Access, Google Scholar, and the ACM Digital Library. The terms to be used for searching were "quantum cryptography," "post-quantum cryptography," "quantum key distribution (QKD)," "quantum computing," and "secure communication." Since a review of only the most recent developments on the subject of interest was intended, only peer-reviewed journal articles dating from 2020 to 2024 were selected for review.

B. Inclusion criteria

The following types of articles have been included in the review:

- Quantum and post-quantum cryptography are reviewed in journal articles to achieve secure communications.
- Research with empirical results, theoretical models, or significant advancements in quantum and post-quantum cryptographic algorithms.
- Manuscripts on challenges, limitations, and future directions of quantum security and post-quantum security systems.

C. Exclusion criteria

The following types of articles have been excluded in the review:

- Studies unrelated to cryptography or secure communications.
- Papers on quantum computing unrelated to areas such as quantum chemistry and quantum machine learning.
- Studies published in non-peer-reviewed outlets and those published before 2020.
- Further, works for which full texts could not be accessed, even after multiple requests to the corresponding author, were also excluded from review.

D. Article Screening and Selection Process

In the systematic search process, 250 papers were uploaded to Mendeley, a reference management software. An automatic duplicate detection was run, revealing 63 duplicates, which, after removal, left 187 unique articles for screening. The titles and abstracts were then manually reviewed for the relevance of each study with regard to quantum and post-quantum cryptography. This initial check for relevance then shortlisted 93 articles that needed to be reviewed in full text. The strict application of the inclusion and exclusion criteria was then followed during the full-text examination. Papers lacking significant cryptographic content, whose main themes were not related to quantum and post-quantum cryptography, or which were published outside the 2020-2024 period were excluded from this review. 40 peer-reviewed articles that would serve as the foundation for this literature review and that formed relevant contributions to the changing landscapes of quantum and post-quantum cryptography were then identified.

E. Quality Assessment

The theoretical papers needed to be screened for rigor and their contributions to the field of quantum and post-quantum cryptography. The following aspects were reviewed for each paper:

- Clarity of Theoretical Framework: Each study was analyzed regarding the strength and coherence of its theoretical model. A clear and structured theoretical framework was preferred since it would allow propositions to be followed easily with logical consistency.
- Contribution to the field: The novelty of the theoretical development pertained to either quantum or post-quantum cryptography. It included those studies that introduced new concepts or better models developed for their most relevant contributions to the studies on secure communication.
- The credibility of the publication outlet: Preference was given first to papers whose publication appeared in high-impact, peer-reviewed journals, recognized based on their contributions to cryptography and information security. This ensured that theoretical models discussed within the document were critically reviewed by experts in the same field.
- Relevance to Secure Communication: Papers that did not contribute directly toward quantum or post-quantum cryptographic methods or their application to secure communication have been excluded. This has ensured that only highly relevant studies were included in this review.

F. Data Extraction and Synthesis

Data extraction in this literature review was performed from theoretical papers, focusing on the main aspects of cryptographic algorithms and frameworks. A structured approach was used to identify and capture the key information of each paper with respect to which cryptographic algorithms were discussed, such as QKD, lattice-based, and hash-based approaches; which underlying security models were considered, including quantum versus post-quantum security assumptions; and which limitations or challenges were pointed out by the authors, including but not limited to scalability issues, computational efficiency, and/or implementation challenges.

These data were then synthesized into a holistic narrative that shows the various contributions of approaches to the development of secure communication systems in the light of a quantum era. Rather than being a statistical meta-analysis, the synthesis was represented as recurring themes, emerging trends, and significant research gaps. The progress and limitations of quantum and post-quantum cryptography were compared and contrasted by the various contributions provided

by different theoretical models. This approach allowed a general understanding of the current state of this field, but future research directions in the combination of quantum and post-quantum approaches into hybrid systems to enhance security were also pointed out.

IV. Literature Review

A. Quantum Computing

Some of the unique principles of quantum physics, such as superposition and entanglement, are harnessed by quantum information science to process and perform information transmission in ways that are completely impossible with classical systems [9]. Complicated problems that include factorization of large numbers and brute-force searching at speeds uncontemplated by classical computers are solved by quantum computers using such principles [9]. Therefore, the rapid development of quantum hardware such as QKD networks has been driven by this development from academia to industry.

A revolutionary paradigm based on the concept of qubits is represented by quantum computing. Superposition—a state of being 0 and 1 at the same time—can be gained by qubits [9]. Hence, huge amounts of information can be processed simultaneously [9]. This enables the processing of huge amounts of information in parallel. As a result, the computational power of quantum computers is increased exponentially with each additional qubit, whereas this happens linearly in classical computers [9]. Significant implications are posed by quantum computing in fields related to cryptography, optimization, machine learning, and more. Opportunities and risks, especially in cryptography, are posed by its ability to efficiently solve previously intractable problems.

Basic Principles:

- Superposition: A number of states are represented by qubits all at once, thus making computation faster [10].
- Entanglement: Correlations useful in operations impossible to classical physics can be represented by entangled qubits [10].
- Quantum gates: The stats of qubits are operated on by quantum gates. The preservation of superposition and entanglement allows quantum algorithms to be outperformed by any classical algorithm [10].

Quantum computing is considered to threaten a set of public key cryptosystems widely used—for instance, the RSA algorithm and elliptic curve cryptography—built on the basis of problems hard for classical computers, such as factoring large numbers [9]. These cryptosystems are solved in polynomial time by quantum algorithms, for example, Shor's algorithm, thus compromising the security of these protocols [9]. It is with classical cryptography, such as Transport Layer Security, that the security of the classical communication protocols is broken by quantum computers. This would include the designing of concrete quantum communication protocols with engineered security, made possible by quantum cryptography. One simple example can be changes in states within QKD to identify a potential eavesdropper [11]. While very promising, general deployment is said to remain in its infancy.

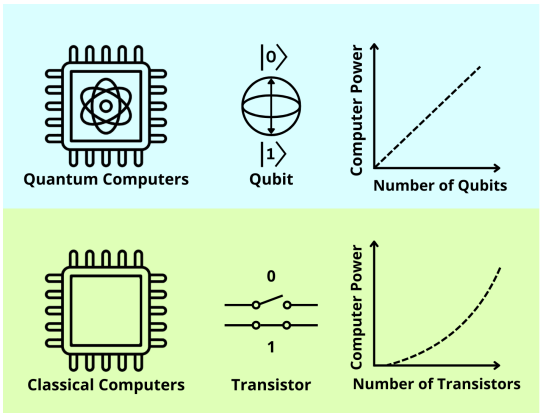

Fig. 1. The computational capacity of conventional and quantum computers is compared. The quantum state is represented as $|\cdot\rangle$ [11].

B. Quantum Cryptography

Quantum cryptography has been recognized as a complete turnaround in secure communications; it depends on the very basis of quantum mechanics to devise cryptographic systems that are intrinsically impossible to intercept [12]. At the very center of this new discipline is QKD, which enables cryptographic keys to be shared by two parties in such a way that any illegitimate attempt at access is immediately detectable [12]. At its core, quantum cryptography is based on the realization that classical cryptography, grounded on computational complexity, steadily becomes more vulnerable with the enhancement of quantum computing. An efficient method for solving mathematical problems like the factorization of integers, is provided by algorithms like Shor's algorithm, which is the basis for the security of RSA and Diffie-Hellman protocols in current usage [9]. Furthermore, one of the most important quantum algorithms, Grover's search algorithm, is highly applicable to symmetric encryption systems like the Encryption Standard (DES) and the Advanced Encryption Standard (AES), as the brute-force key search is substantially accelerated [11]. With Grover's algorithm, the DES could be broken with many fewer operations compared to what could be achieved by any classical approach [11]. In contrast, QKD is applied to key distribution in such a way that the resulting keys cannot be cracked by any computational power, even those belonging to quantum computers [12]. The well-known protocol known as BB84, introduced by Bennett and Brassard in 1984, is considered the earliest and most famous QKD protocol [11]. The principle that any attempt at measurement will disturb the quantum states of particles like photons is the basis of this protocol [9]. This is an inherent property that provides the possibility of detecting the presence of an eavesdropper, conventionally referred to as Eve, at the moment of transmission, while the communicating parties are conventionally referred to as Alice and Bob [11]. If the quantum key is intercepted by Eve, the state of the particles will be disturbed by her measurement, consequently alerting Alice and Bob to potential security breaks [11]. A

number of key advantages over classical approaches are offered by quantum cryptography. First, its information-theoretic security ensures that any third-party acquisition of knowledge about the shared key will necessarily be detected, making it fundamentally more secure than traditional systems [13]. This sharply contrasts with classical cryptography, which is based on the assumption that some mathematical problems are hard to solve—an assumption falsified in principle by quantum algorithms.

C. Quantum Secure Communication

Quantum secure communication is regarded as a quantum leap in cryptography, being based essentially on the very ground of quantum mechanics for setting up a level of security that could never have been envisaged classically [2]. It is rooted in QKD, allowing a shared secret key to be generated between two parties, Alice and Bob, in a way that makes the process resistant to eavesdropping by Eve, due to the fundamental properties of quantum states [14], [13], [15]. It was shown by the seminal BB84 protocol that security could be based on the laws of quantum mechanics rather than on computational difficulty [11]. The unconditional security paradigm of QKD guarantees against interceptions—in fact, any such attempt at interception can be detected—a feature that is quite out of reach for any classical cryptographic system [11], [16], [17]. Advances have been made in device-independent QKD, which solves the issues of untrusted devices and consolidates quantum communication protocols for robustness [16]. With the further development of this science, key management, error correction, and privacy amplification are gaining vital importance so that practical implementation with quantum secure communication may have a minor compromise on security [11], [17], [18]. A deep insight into the basic concept, protocols, and recent developments in quantum secure communications is given in this chapter to set the groundwork for understanding its critical role in the near future of secure information exchange.

QKD protocols are mainly divided into two classes: prepare-and-measure protocols and entanglement-based protocols [19].

- More specifically, the well-known prepare-and-measure protocols, such as BB84, are based on the preparation of quantum states by Alice and their measurement by Bob, while that class of protocols relies on the fact that any attempt at eavesdropping necessarily introduces detectable disturbances [19].
- In entanglement-based protocols, such as E91, entangled pairs of particles are used for key exchange [19]. The implementation of these protocols is considered more complex, and an increase in security is allowed due to properties featured by quantum entanglement [19]. Security key distribution is provided by both types of protocols owing to the use of fundamental principles of quantum mechanics for the detection of possible attempts at eavesdropping [19].

QKD systems are divided into two major classes: Discrete-Variable QKD (DV-QKD) and Continuous-Variable QKD (CV-QKD) systems [20], [13].

- In the case of the DV-QKD system, information is encoded onto discrete quantum states, which normally correspond to the polarization of single photons, and special equipment such as single-photon sources and detectors is usually required [13]. The well-noted protocols prepared to measure polarized photons using specific bases include BB84, Ekert91, and BBM92 [13].
- In CV-QKD, information is encoded into the continuous variables of electromagnetic fields, such as the conjugate quadratures of light, and these quadrature components are modulated using secret key bits [20], [13]. The clearest advantages of CV-QKD include operational simplicity, potential for higher transmission rates, and compatibility with existing coherent optical communication infrastructure [20]. It is also represented as an experimental alternative offering high secret key rates at possibly much lower costs, particularly for short-distance transmission. [13]. On the other hand, range limitations in optical fiber transmission are suffered by CV-QKD unless quantum repeaters become viable [13]. To this end, much attention has been received by air-based (free space) communication of CV-QKD, particularly for long-distance applications where satellite-based global quantum communication is considered due to the low attenuation of air within a few transmission windows [20].

The BB84 protocol is regarded as providing the inspiration for most other QKD protocols [21]. It is a prepare-and-measure protocol, where quantum states are prepared by a sender (Alice) and measured by a receiver (Bob) [19]. In the BB84 protocol, each bit of Alice's message is encoded randomly in one of two non-orthogonal bases, usually the rectilinear and diagonal bases [21], [15]. Polarized photons act as qubits to encode the information, where logic 0 and 1 correspond to a photon polarized at 0° and 90°, respectively, in the rectilinear basis, and logic 0 and 1 correspond to a photon polarized at 45° and 135° in the diagonal basis [15]. The received quantum states are measured by Bob in a random choice of one of the two bases in each measurement [21]. After the quantum transmission is complete, classical communication is initiated between Alice and Bob by comparing the bases they had chosen; all the bits measured in different bases are removed, keeping only the matched pairs in order to generate the shared key [21]. This key sifting described here is thought of as indispensable for any security guarantee of the generated key. In the BB84 protocol, two basic principles of quantum mechanics, on which security is based, are the no-cloning theorem and the probabilistic character of quantum measurements [22]. In fact, detectable anomalies will necessarily be introduced by any attempt to intercept the quantum states [19].

The major indicator used to trace the eavesdropping in BB84

is the Quantum Bit Error Rate (QBER), which is defined as a ratio between the number of invalid received qubits and the total number of qubits that are sent [22]. Mathematically, QBER is expressed as:

$$\text{QBER} = \frac{N_{\text{error}}}{N_{\text{total}}} \tag{1}$$

where N_{error} is defined as the number of qubits received by Bob with errors, and N_{total} is defined as the total number of qubits sent by Alice [22]. For the detection of eavesdropping, a QBER comparison algorithm with the threshold θ_{QBER} is used by Alice and Bob [22]. If the measured QBER is found to be higher than the threshold, a potential eavesdropping attack is indicated [22]:

$$\text{QBER} > \theta_{\text{QBER}}, \quad \text{Eavesdropping Detected} \tag{2}$$

Decoy-state BB84 was designed to handle some realistic problems that are usually faced in generating single photons [14]. Decoy-state BB84 was designed to handle some realistic problems that are usually faced in generating single photons [14]. Firstly, it is pretty challenging to reliably generate true single-photon sources [14]. The new version allows for weak laser pulses to be sent by Alice instead of a single photon, thereby providing an important improvement in the security of the protocol against some attack vectors, such as the Photon-Number-Splitting (PNS) attack [14]. The key rate in decoy-state BB84 protocol is dependent on noise levels, losses, and intensity of laser pulses [14]. The key rate R of the decoy-state BB84 can be expressed in terms of the number of detection events N, the error rate E ,and the average intensity of the laser pulses μ as [14]:

$$R = f(N, E, \mu) \tag{3}$$

The function f is dependent on the interplay of these parameters, which dictates the secure key rate [14]. In essence, the key rate R is diminished by an increasing error rate E and losses in detection events, while careful tuning of μ helps to optimize the performance of the protocol against attacks such as PNS attacks [14].

The E91 protocol, introduced by Artur Ekert in 1991, is registered as another significant QKD protocol that relies on quantum entanglement—a distinctive differentiating property compared to other protocols like BB84, which rely on the no-cloning theorem [9]. Similar to the BB84 protocol, it is consisted of three main steps: raw key exchange, key sifting, and key distillation [21]. More precisely, in the E91 protocol, a stream of entangled pairs of quantum particles is produced by a particular photon source [21]. One photon from each pair is received by Alice and Bob through a quantum channel [21]. Their respective photons are observed by each of them, with measurement bases selected independently and randomly, while the time, basis, and outcomes of each measurement are recorded [21]. Surprisingly, it is not necessary that Alice and Bob be directly linked by a quantum channel [9]. Instead, it could be that entangled qubit pairs are prepared and then arbitrarily separated [9]. Subsequently, measurements are taken, the information is compared classically, and the bits measured with different bases are discarded [21]. This protocol's key efficiency is considered low, at about 22%, as out of nine possible combinations of bases, only in two cases result in Alice and Bob using the same bases [9]. In the key reconciliation step, Bell's inequality test is employed to check for eavesdropping by analyzing the correlation in the measurements made with different bases [21], [9]. In respect of its special detection of the presence of an eavesdropper, together with its use of quantum entanglement, the E91 is considered among the most important protocols in quantum secure communications [21].

Quantum secure communication, particularly QKD, is recognized as a revolutionary new class of cryptographic techniques that are based on the exploitation of fundamental principles of quantum mechanics to offer unparalleled levels of security [12]. From the seminal BB84 protocol to more advanced implementations such as DV-QKD and CV-QKD and entanglement-based protocols such as the E91 protocol, immense progress has been carried out so far. These protocols, therefore, offer security guarantees based not on computer complexity but on the laws of physics. Key management, error correction, and privacy amplification are considered increasingly less difficult to carry out while the technology is maturing, and practical implementations have become feasible. Other areas of research are Device-Independent QKD and free-space quantum communication as a means of enhancing the reliability of such systems, along with the distances involved [20]. Quantum secure communication will remain the core of sensitive information protection in an ever-connected world.

D. Challenges in Quantum Cryptography

In recent years, quantum cryptography has been considered a very promising area of secure communications in the quantum era, especially QKD. However, despite the theoretical guarantees of security, numerous obstacles are faced in the practical implementation of quantum cryptography. The purpose of this chapter is to investigate those challenges based on recent literature.

- **Implementation Complexity and Hardware Limitations**: Implementation complexity and hardware limitations are faced due to the reliance on accurate management of quantum communication instruments and channels [19]. Special machinery is also needed in the development and maintenance of communication channels, key generators, and quantum repeaters, hence incurring high costs [19], [23]. The one-photon detector, important in recognizing quantum cryptography signals, is considered resource-intensive with low noise tolerance, hence a big obstacle to mainstream adaptation [23].
- **Channel Loss and Noise**: Channel loss and noise are suffered by QKD in practical scenarios. These two factors are highly sensitive and have a great tendency to introduce errors and reduce the communication range [19]. The existence of environmental noise, for example,

within power systems, makes reliable operations of QKD systems challenging [21].

- **Distance Limitations**: The working range of QKD systems is very limited because of quantum signals' extreme attenuation across extremely vast distances [19]. Experimental investigations have already demonstrated that major challenges are faced by the QKD protocols in performing beyond 300 km without a drastic reduction in the key rate [21].
- **Quantum Error Correction**: Quantum errors are induced by external influences, compelling the development of quantum fault tolerance and, hence, mechanisms for error correction [23]. Thermal impulses, electromagnetic influences, defects in detectors, photo loss, and decoherence all raise the rate of errors in quantum systems [23]. The speed at which keys are generated using quantum cryptography is reduced by error correction [23].
- **Authentication Challenges**: While symmetric cryptographic keys are established by QKD, the process itself does not intrinsically authenticate the identities of the communicating parties [21]; hence, the use of some extra classical authentication protocols or post-quantum cryptographic techniques is absolutely required to ensure the legitimacy of the communication parties [21].
- **Integration with Classical Infrastructure**: While the quantum networks are integrated into the existing classical infrastructure, such as intranets and other communication networks, the process of establishing trust becomes highly complicated [9]. The existence of any type of vulnerability in the classical infrastructure makes the quantum network security vulnerable, therefore making the process of integration more challenging [9].

E. Post - Quantum Cryptography

With a higher dependency on digital systems being taken by the modern world, a rising demand for strong cryptographic mechanisms resistant to new emerging technological challenges is also noted. In this respect of security, post-quantum cryptography (PQC) is positioned well at the frontiers, aimed at any vulnerability threatened by quantum computing against contemporary cryptographic systems [24], [25]. PQC emerged as a response to the potential threat that traditional cryptographic systems face from quantum computers [24], [25]. Unlike quantum cryptography, which has its security relied upon properties of quantum mechanics, classical cryptographic systems that are resistant to both conventional and quantum computer attacks are sought to be developed by PQC [25], [26]. Thus, the development of PQC is based on an important realization that many popular cryptographic protocols—in particular, those relying on public-key cryptography—might become vulnerable to a sufficiently powerful quantum computer [24] , [27]. It is this realization that has built up a movement in the research community toward the development of new cryptographic primitives and protocols that can retain security in the post-quantum world. In general, the goal of PQC is to devise mathematical problems that would remain beyond the computational powers of quantum computers [26]. The very foundation of cryptography is dependent upon it, while new mathematical structures and problems are investigated to provide resilience to quantum attacks [26]. In other words, the development of PQC is pursued along multidisciplinary lines to integrate advanced mathematics, computer science, and cryptography [26]. In this regard, multiple mathematical bases are considered, each coming with certain properties that could enact robust security in a post-quantum world [26]. The development of post-quantum cryptography is recognized as having significant global ramifications for the security of information, not merely as an academic exercise. Since quantum computing technology rapidly advances, a need for quantum-resistant cryptographic systems has been identified to protect sensitive data and communication [24], [27]. Developments in PQC are being closely followed by industries such as finance, health, governments, and defense in a manner that shows their interest in the safeguarding of their long-term security [27].

This setup has been prepared for the immediate development of quantum-resistant cryptography. Extensive research efforts are being conducted globally, along with standardization processes. The forefront of these respects has already been taken by the National Institute of Standards and Technology (NIST), where the standardization process of post-quantum cryptography was launched in 2016 [26]. Already, several promising candidates for standardization have resulted, providing a strong indication of progress in this area [26]. The successful implementation of post-quantum cryptography will be required for digital information to remain confidential, intact, and authentic over the next couple of decades.

F. Types Of Post-Quantum Cryptography

PQC was referred to by an assortment of cryptographic systems typed for resistance against attacks that utilize both classical and quantum computers [25]. These schemes are based on mathematical problems that are presumably considered difficult even for quantum algorithms.

- **Lattice-based cryptography (LBC)**: One of the most promising areas in PQC is considered to be LBC, as it is based on computational hardness problems for lattices, including the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which are perceived to be NP-hard and resistant to quantum attacks [28]. The benefits of LBC, including efficiency and scalability, are exploited in a wide range of applications, including secure communication protocols like HTTPS and TLS [28]. Some well-known implementations, including Frodo, NTRU, New Hope, and Kyber, have been developed [29]. The Ring Learning With Errors problem is formed as the foundation of the majority of LBC strategies [26]. Despite these features, very large keys, typically several thousand bits, are required by lattice-based systems [30]. However, ongoing research is being conducted to enhance the performance of these systems, which is expected to increase their practical use in real-world applications.

- **Code-based cryptography (CBC)**: CBC is considered one of the most promising candidates regarding decoding a random error-correcting code in the PQC arena [28]. The security, based on the NP-hard syndrome decoding problem, depends on the identification of an error vector of small hamming weight for a given syndrome vector and a parity check matrix [31]. The McEliece cryptosystem was proposed in the year 1978, laying down the fundamental building blocks for code-based cryptography [32]. Goppa codes are used to impose random errors upon the encryption, and these errors are subsequentially removed during decryption [28]. Another popular implementation is the Niederreiter cryptographic scheme, which is considered a variation of the McEliece and is noted to offer faster performance while maintaining similar security properties to its predecessor [26]. CBC schemes are noted for being extremely fast at the encryption and decryption stage but are afflicted by key-size issues, ranging from 100 KB to several MB [30]. Different variants have been proposed by experts to overcome these key size issues, such as the Courtois-Finiasz-Sendrier signature scheme, SURF scheme, and Wave signature scheme [31].
- **Multivariate cryptography (MC)**: MC copes with nonlinear systems of equations over finite fields and is able to classify this problem as NP-hard [28]. These systems mainly utilize multivariate quadratic polynomials, which are designed to resist quantum attacks [28]. The Patarin's Hidden Fields, Unbalanced Oil and Vinegar Cryptosystems, Rainbow, and Hidden Field Equations are based on these principles [28], [29], [26]. The relative advantages of multivariate cryptography are noted to include short signatures, therefore making them faster [26]. The disadvantage of multivariate cryptography is that it is considered very slow during decryption, apart from its large key sizes [30]. The inclusion of slow decryption speeds and large key sizes brings challenges that will need to be addressed by future improvements for better efficiencies to be achieved [30].
- **Hash-based cryptography (HBC)**: HBC leverages the concept of one-time signature—a concept whereby every message that is to be signed is supposed to have one key pair associated with the signature process [28]. This technique is based on the hash functions underlying the one-way function, making it one of the simplest notions [26]. To address the one-time signature's (OTS's) vulnerability related to the reuse of the key pair, the Merkle scheme uses binary hash trees, with OTS public key hash values arranged as leaf nodes, which enables secure key management using collision-resistant hash functions [28]. The ones that come under this category include the Extended Merkles Signature Scheme (XMSS), Lamport signatures, and SPHINCS+ [26]. Although security is guaranteed in these kinds of signatures, sometimes the use of large keys and signature sizes restricts its applications [26].
- **Isogeny-based cryptography (IBC)**: IBC, stands for supersingular elliptic curve isogeny cryptography, which is considered one of the newer arrivals in the PQC landscape [29]. The idea here lies in the construction of isogenies among supersingular elliptic curves [29]. The difficulty of identifying an isogeny between two given elliptic curves is determined by the security of isogeny-based systems [25]. Examples of these systems include Supersingular Isogeny Diffie-Hellman (SIDH), Supersingular Isogeny Key Encapsulation (SIKE), and Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) [29], [26]. Most of these isogeny-based systems are actually challenging with respect to key sizes. For example, according to some estimates, the public key size of the SIKEp434 scheme alone has been said to be 2640 bits [30].

G. Threats to Post-Quantum Cryptography

Cryptographic systems have indeed been furnished by quantum computing, and anxieties have been raised with respect to the robustness of PQC solutions. Though resistance against quantum-based attacks was designed into many of these systems, vulnerability is actually present in many of them due to quantum and classic algorithmic improvements. Continuous reconsideration and reinforcement in the case of PQC systems are needed for these threats. Similar to its classical counterpart, PQC is still considered vulnerable to advances in quantum-based and classical algorithms [27]. Indeed, the security of many PQC schemes, including code-based, multivariate, and isogeny-based cryptosystems, has so far been implicated by some of these specific proposals of algorithms [27]. Among these, a number of candidate algorithms have been flagged by NIST, including Bit Flipping Ky Encapsulation, Hamming Quasi-Cyclic, and SIKE, which have been found to be vulnerable to quantum attacks [27]. The young age and limited amount of research into PQC cryptosystems make them still vulnerable to quantum or classical threats [27]. The vulnerabilities of PQC schemes are limited by the other aspects of the limited exploration into breakthroughs in cryptanalysis. The evolving problem of the quantum threat to PQC is concerned with new methods of cryptanalysis that may emerge with improvements in quantum computing.

H. Synergy of Quantum and Post-Quantum Cryptography

The integration of QKD and PQC is seen as ushering in a promising frontier in cryptographic studies that tries to leverage the respective strengths of the approaches while mitigating their individual weaknesses.

One of the central ways of unifying QKD and PQC is made through the concept of joint cryptosystems [33]. Such systems are generally designed to improve the security and practicality of QKD by having elements from the PQC side incorporated, mostly within the information reconciliation phase [33]. One of the most interesting developments involving joint QKD-PQC systems is the use of PQC algorithms for encrypting the parity bits sent out during the error correction phases of QKD [33]. This approach could limit the leakage of information in error reconciliation, as the syndrome vector is encrypted

with a PQC algorithm and the transmission distance of QKD is extended, possibly with an increased secret key generation rate [33]. High-rate Low-Density Parity-Check (LDPC) codes are applied for information reconciliation, where (N - K) is less than the number of secure bits of the PQC system [33]. Here, N is defined as the total number of bits in the encoded message, including both the original data bits and the parity bits, while K is defined as the number of original data bits being encoded [33]. This scheme is designed to avoid information leakage due to parity-bit transmissions over an authenticated public channel, which occurs in traditional QKD protocols [33]. In a practical implementation of this concept, for instance, a McEliece cryptosystem based on quasi-cyclic LDPC coding could be integrated within the QKD protocol [33]. This is regarded as quite attractive because the complexity of the realization would be reduced, and realizations of the hardware of LDPC encoder and decoder in Field-Programmable Gate Arrays already exist [33].

One more synergy possible between QKD and PQC is found in the application of QKD to improve the security of PQC protocols, especially concerning potential quantum attacks in the future [34]. The initialization stages of the cryptographic protocol can have QKD applied [34]. In this case, instead of having QKD make use of generating keys all along, initial secure sequences are generated by QKD [34]. These sequences can be utilized for generating secure sequences of public keys, providing seeds for random "hash function" generators, and more simple protocol parameter initialization [34]. This approach solves the problem of the low key rates of QKD systems, as much shorter initialization sequences can be utilized than those imposed by one-time pad encryption [34]. One such concrete implementation is seen in the enhancement of lattice-based cryptography [34]. For instance, the public matrix A and parameter q in Learning With Errors schemes can have seeds shared by QKD in such a way that these critical elements are used only once [34]. The protocol may be rendered resistant to future quantum computer attacks even when sophisticated algorithms for efficient matrix inversion, such as Harrow-Hassidim-Lloyd algorithm, are employed [34].

Most of the challenges posed by the integration of QKD and PQC relate to widespread adoption. Complexity is identified as one major challenge since management and maintenance challenges will be posed by the use of joint systems in hardware and software implementations [33]. This highly sophisticated infrastructure is also hard to scale [33]. A second challenge is associated with the rigorous security proofs required in such hybrid systems. Further theoretical work is needed to ensure that the highest security standards are met by the combined approach of QKD and PQC [33].

V. Future Directions

As the fields of QKD and PQC continue to advance, it is expected that several directions will take center stage in the coming years of research and development. The main directions for further development of these technologies are discussed in this chapter.

- **Quantum Internet Infrastructure**: While quantum Internet infrastructure is not foreseen for anytime soon, it also serves as motivation for many research efforts [9]. The development of both hardware and software infrastructures for quantum protocols and the research on the possibility of wireless quantum secure direct communication will be involved [9].
- **Hybrid Systems and Integration**: The development of hybrid systems, including classical, post-quantum, and quantum technologies, is considered to have a very promising future direction in the hybrid models that are expected to reconcile setup phases, the management of pre-shared values, and key storage for more nodes [35].
- **Advanced Quantum Hardware and Algorithms**: The sustained advancement of quantum hardware is thought to be the keystone for progress to be realized in both PQC and QKD [36]. A process involving the fundamental study of quantum materials, electronic advances, and transistors, among others, at the heart of information and communication technologies is involved here [36]. The greater the improvement in quantum hardware, the greater the effort that will be needed in the development and perfection of quantum algorithms that make use of such an improvement [26].
- **Quantum Cybersecurity and Warfare**: Research on quantum cybersecurity, attack, and warfare is expected to become increasingly important to quantum technology advances [36]. Designing against quantum attacks and extending quantum technologies for application in national security contexts is entailed [36].

VI. Conclusion

Where opportunities are brought by quantum computing, some challenges are also brought to cryptography in general, and most notably to quantum-resistant encryption systems. A very secure approach based on principles of quantum mechanics is represented by QKD; however, the same crucial drawbacks are suffered by it: a short-distance transmission and low key generation rates confine it. A broader area, PQC, is represented by quantum-resistant cryptography. More scalable solutions based on mathematical problems that are infeasible to solve, both for classical and quantum attacks, are offered by PQC. Hybrid systems, which will try to use the strengths of both QKD and PQC in order to overcome the weaknesses, will be attempted. Still, some challenges remain in the infancy of PQC, practical challenges due to constraints of distance, and infrastructural complexity. Important research issues in cryptography within the near future will remain quantum Internet infrastructure, quantum communication protocols and hardware, and quantum cybersecurity and warfare studies. In the future, successfully combining quantum and post-quantum technologies would be the focus of cryptography since the new frontier of cryptography is considered to be represented by both scientific processes. As these technologies are refined by research studies and their weaknesses are overcome, this

dream will be driven even closer to the development of practical, scalable quantum-secure communication systems.

VII. Acknowledgment

Gratitude is expressed to Mr. Amila Senarathne, Senior Lecturer in the Department of Computer System Engineering at the Sri Lanka Institute of Information Technology, whose guidance was instrumental in navigating the journey of writing this review paper.

References

[1] S. S. Gill and R. Buyya, "Transforming research with quantum computing," *Journal of Economy and Technology*, 2024.

[2] P. G. Jackson, A. Thakur, and K. Kaur, "Quantum cryptography," *SSRN Electronic Journal*, 2024. Available at SSRN: https://ssrn.com/abstract=4916293 or http://dx.doi.org/10.2139/ssrn.4916293.

[3] R. Bavdekar, E. Chopde, A. Bhatia, K. Tiwari, S. Daniel, and Atul, "Post quantum cryptography: Techniques, challenges, standardization, and directions for future research," 02 2022.

[4] C. Ugwuishiwu, U. Orji, C. Ugwu, and C. Asogwa, "An overview of quantum cryptography and shor's algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, p. 7487 – 7495, 07 2021.

[5] S. Hoque, A. Aydeger, and E. Zeydan, "Post-quantum secure ue-to-ue communications," 2024.

[6] E. Dervisevic, A. Tankovic, E. Fazel, R. Kompella, P. Fazio, M. Voznak, and M. Mehic, "Quantum key distribution networks – key management: A survey," 2024.

[7] M. Kumar, "Post-quantum cryptography algorithm's standardization and performance analysis," *Array*, vol. 15, p. 100242, 2022.

[8] M. Page, J. Mckenzie, P. Bossuyt, I. Boutron, T. Hoffmann, C. Mulrow, L. Shamseer, J. Tetzlaff, E. Akl, S. Brennan, R. Chou, J. Glanville, J. Grimshaw, A. Hróbjartsson, M. Lalu, T. Li, E. Loder, E. Mayo-Wilson, S. Mcdonald, and D. Moher, "The prisma 2020 statement: an updated guideline for reporting systematic reviews," *Systematic Reviews*, vol. 10, 03 2021.

[9] Z. Yang, M. Zolanvari, and R. Jain, "A survey of important issues in quantum computing and communications," *IEEE Communications Surveys Tutorials*, vol. 25, no. 2, pp. 1059–1094, 2023.

[10] H. A. Bhat, F. A. Khanday, B. K. Kaushik, F. Bashir, and K. A. Shah, "Quantum computing: Fundamentals, implementations and applications," *IEEE Open Journal of Nanotechnology*, vol. 3, pp. 61–77, 2022.

[11] D. Pan, G.-L. Long, L. Yin, Y.-B. Sheng, D. Ruan, S. X. Ng, J. Lu, and L. Hanzo, "The evolution of quantum secure direct communication: on the road to the qinternet," *IEEE Communications Surveys & Tutorials*, 2024.

[12] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, *et al.*, "Quantum key distribution: a networking perspective," *ACM Computing Surveys (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[13] D. Pan, K. Li, D. Ruan, S. X. Ng, and L. Hanzo, "Single-photon-memory two-step quantum secure direct communication relying on einstein-podolsky-rosen pairs," *IEEE Access*, vol. 8, pp. 121146–121161, 2020.

[14] T. Attema, J. W. Bosman, and N. M. Neumann, "Optimizing the decoy-state bb84 qkd protocol parameters," *Quantum Information Processing*, vol. 20, no. 4, p. 154, 2021.

[15] C. Biswas, M. M. Haque, and U. Das Gupta, "A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography," *IEEE Access*, vol. 10, pp. 72743–72757, 2022.

[16] R. Arnon-Friedman and F. Leditzky, "Upper bounds on device-independent quantum key distribution rates and a revised peres conjecture," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6606–6618, 2021.

[17] M. Wazid, A. K. Das, and Y. Park, "Generic quantum blockchain-envisioned security framework for iot environment: Architecture, security benefits and future research," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 248–267, 2024.

[18] M. Khawasik, W. Elsayed, M. Rashad, and A. Younes, "A secured quantum two-bit commitment protocol for communication systems," *IEEE Access*, vol. 10, pp. 50218–50226, 2022.

[19] S. Bajrić, "Enabling secure and trustworthy quantum networks: Current state-of-the-art, key challenges, and potential solutions," *IEEE Access*, vol. 11, pp. 128801–128809, 2023.

[20] M. Li and T. Wang, "Continuous-variable quantum key distribution over air quantum channel with phase shift," *IEEE Access*, vol. 8, pp. 39672–39677, 2020.

[21] P.-Y. Kong, "A review of quantum key distribution protocols in the perspective of smart grid communication security," *IEEE Systems Journal*, vol. 16, no. 1, pp. 41–54, 2022.

[22] C. Lee, I. Sohn, and W. Lee, "Eavesdropping detection in bb84 quantum key distribution protocols," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2689–2701, 2022.

[23] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1092–1101, 2024.

[24] D. Chaudhary, U. Kumar, and K. Saleem, "A construction of three party post quantum secure authenticated key exchange using ring learning with errors and ecc cryptography," *IEEE Access*, vol. 11, pp. 136947–136957, 2023.

[25] F. Borges, P. R. Reis, and D. Pereira, "A comparison of security and its performance for key agreements in post-quantum cryptography," *IEEE Access*, vol. 8, pp. 142413–142422, 2020.

[26] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro, and A. Erbad, "A survey and comparison of post-quantum and quantum blockchains," *IEEE Communications Surveys Tutorials*, vol. 26, no. 2, pp. 967–1002, 2024.

[27] K. F. Hasan, L. Simpson, M. A. R. Baee, C. Islam, Z. Rahman, W. Armstrong, P. Gauravaram, and M. McKague, "A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies," *IEEE Access*, vol. 12, pp. 23427–23450, 2024.

[28] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157356–157381, 2020.

[29] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava, R. Matulevičius, A.-A. O. Affia, M. Laurent, N. H. Sultan, and Q. Tang, "Post-quantum era privacy protection for intelligent infrastructures," *IEEE Access*, vol. 9, pp. 36038–36077, 2021.

[30] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21091–21116, 2020.

[31] Y. Lee, W. Lee, Y. S. Kim, and J.-S. No, "Modified pqsigrm: Rm code-based signature scheme," *IEEE Access*, vol. 8, pp. 177506–177518, 2020.

[32] M. R. Nosouhi, S. W. A. Shah, L. Pan, and R. Doss, "Bit flipping key encapsulation for the post-quantum era," *IEEE Access*, vol. 11, pp. 56181–56195, 2023.

[33] I. B. Djordjevic, "Joint qkd-post-quantum cryptosystems," *IEEE Access*, vol. 8, pp. 154708–154712, 2020.

[34] I. B. Djordjevic, "Qkd-enhanced cybersecurity protocols," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–8, 2021.

[35] S. Ricci, P. Dobias, L. Malina, J. Hajny, and P. Jedlicka, "Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography," *IEEE Access*, vol. 12, pp. 23206–23219, 2024.

[36] A. Kumar, S. Bhatia, K. Kaushik, S. M. Gandhi, S. G. Devi, D. A. De J. Pacheco, and A. Mashat, "Survey of promising technologies for quantum drones and networks," *IEEE Access*, vol. 9, pp. 125868–125911, 2021.

B. D. Anuththara Divyanjalie Hettiarachchi , a final-year undergraduate student at the Sri Lanka Institute of Information Technology, Sri Lanka, within the Department of Computer Science, following a B.Sc. (Hons) in Information Technology Specializing in Data Science. Her research interests encompass data science, focusing on machine learning, deep learning, and artificial intelligence, as well as physics, astronomy, and space science.